

工信部从源头整治虚假诈骗电话——

电信企业要确保主叫号码真实



本报记者
叶薇

山东学生徐玉玉、宋振宁相继遭遇电信诈骗，伤心欲绝而亡；网传清华大学老师卖房后刚到账1760万元，就被骗子以涉嫌偷漏税款等说辞全部卷走……电信诈骗引发广泛关注。工信部近日表示，将重点从源头整治虚假诈骗电话，要求电信企业确保主叫号码的合法性和真实性。

电信诈骗已成为社会顽疾，从个人信息保护，到实名制登记，再到加大执法力度，从运营商、金融机构、互联网企业到公安机关，无论哪一环有缺漏，都会撞坏社会信息安全的大门。

四种措施 整治篡改来电号

电信诈骗的惯用伎俩是伪造来电号码。针对篡改来电显示或虚假电话号码的几个产生渠道，工信部采取了四种措施：

一是要求电信企业建立语音专线主叫号码鉴权机制，未通过鉴权的呼叫，一律拦截，并对专线用户使用的主叫号码或号段定期查验，确保主叫号码的合法性和真实性。

二是对非法设置VoIP经营平台、非法提供VoIP电话落地及改号服务的企业，依法责令改正、记入信誉档案、向社会公开，情节严重涉嫌违法犯罪的，移交公安部门。同时督促相关互联网企业在搜索引擎、电商平台、应用商店、社交网络等网络空间，通过关键词屏蔽、APP下架等方式，斩断改号软件的网上发布、搜索、传播、销售、宣传等渠道。

三是进一步规范国际主叫号码传送，落实对国际来电中“+86”不规范主叫号码的拦截工作，有效阻断境外非法诈骗电话呼入。同时，面向全国手机用户提供国际来电的甄别和提示服务。

四是进一步打击非法伪基站发送虚假信息。

目前，一些手机厂商已推出多种第三方软件来标记疑似骚扰和诈骗电话，有陌生来电可提前显示电话类型。用户如果判断是诈骗或骚扰电话，可立即拉入黑名单。但厂商各自为政，也容易出现误判。下一步，工信部将大力推动基础电信企业、互联网企业、各手机安全软件企业、手机终端厂商共享骚扰信息标注数据，利用大数据、云计算等技术，预防和处置垃圾短信和骚扰电话。

虚商号段 电信诈骗重灾区

徐玉玉案中，实施诈骗的170/171号段属于虚拟运营商专用号段。在国内电话诈骗案中，虚商号段是重灾区。

2013年，为进一步促进移动通信市场竞争，工信部向民间资本开放了移动通信转售业务试点，并



划分170和171号段供移动转售企业使用，由此产生了一大批虚拟运营商。

从客观上看，民营激发了移动通信市场的活力，但到了去年下半年，虚拟运营快速增长，问题逐渐暴露。有的虚拟运营商对实名制要求落实不到位，被不法分子利用。

今年7月，工信部网络安全管理局对虚商新人网电话用户实名认证工作暗访，并抽测部分虚商在网用户实名认证信息合规率。在暗访的109个网点中，发现37个存在违规行为，违规比高达33.9%。

业内人士李军透露，工信部要求激活手机卡的前提，是当事人的身份证正反面以及手持身份证照片，但这个环节很容易被骗子利用——用假身份证、找一个形似者或购买别人的实名制电话卡，都会对虚商的实名制带来挑战。

通信专家项立刚认为，由于市场小，很多虚拟运营商舍不得投入，仍靠经营语音、流量及发送广告等营利，并没提升服务。加上技术开发程度低，导致实名制迟迟无法实现，为电信诈骗提供了便利。

工信部表示，将把实名制落实情况作为虚拟运营商申请扩大经营范围、增加码号资源、发放正式经营许可证的一票否决项。在整改落实到前，其业务准入、码号核配、扩大经营范围等相关审批一律不予通过。情节严重的，将要求相应基础电信企业暂停启用已核配的码号资源。

电信诈骗等级

入门级：漫天撒网碰运气

成长级：编故事连环诈骗

进阶级：技术伪装，引诱上钩

精通级：确定信源，精准下套

图 CFP

社会合力 独自作战远不够

电信诈骗中，运营商扮演了何种角色？工信部表态称，运营商在治理垃圾短信和骚扰电话方面应承担应有的责任和义务，包括：

一是严格落实手机实名制；二是确保主叫号码正确真实传送；三是规范管理通信线路资源和号码资源；四是及时中止和阻断不法信息的传播。

一些法律专家看来，电信公司对电信诈骗泛滥应承担责，但实际较难解决。电信运营商有义务为客户提供完善服务，不能随意停止某号段甚至某号码的服务，也不能在不符法律法规的要求下泄露号码持有人的具体身份。消费者可以选择选择不接电话，但运营商无权不传输，否则可能涉嫌歧视和违法。根据《电信服务规范》，电信用户全程享有使用通信权，所有公民都有平等接入电信网络，使用电信服务的权利。

对抗无孔不入的电信网络诈骗，单靠某一家机构独自作战是远远不够的，需要社会各界联合起来。通信专家项立刚认为，电信诈骗实际上应该叫通信诈骗或网络诈骗，反通信诈骗是一个综合体系，需要各部门配合。公安机关的打击治理，互联网公司、电信运营商、银行等行业机构的技术对抗，普通用户的有效防范，缺一不可。

贩卖信息已成黑色产业链

电信网络诈骗案件背后，隐藏着一条黑色产业链。包括专门收集、买卖公民个人信息的“信息链”，专门买卖银行卡、帮诈骗分子迅速转移骗款的“资金链”等。

由于没有门槛，贩卖个人信息的不法分子与日俱增。他们开设各类“数据挖掘”“信息咨询”公司，专门倒卖信息，已形成“源头—中间商—非法使用人员”的交易模式，团队作案。有一些专门用于信息买卖的QQ群，如“菠菜”“料主包养”“拦截马”。为了增加隐蔽性，群头像有

时是一堆美女、有时则会标注隐晦的“稳赚计划”“注册有礼”等。

业内人士李军透露，QQ群中，信息被称为“料”，相较于售价几毛钱的身份证、手机信息，兜售支付宝余额“料”和各大银行“料”的人是群里“大户”。比如支付宝“料”，就包括用户登录和支付密码、手机号、身份证号和快捷账号，余额1000元以下的支付宝售价80元、1000至3000元售价150元，额度越高，售价越高，大家均默契地先付款后拿“料”。

本报记者 叶薇

开学季电信诈骗七大陷阱

开学季是电信诈骗多发期。记者采访上海移动等运营商了解到，针对高校学生的各类电信诈骗手段主要有七类——

1. 机票退改签

“XX乘客，您预订的航班因机械故障已取消，请及时联系航班改签退票专线：XXXXXX(改签成功后由民航赔付航班延误险补偿200元整)。”注意，任何涉及退款或汇款的短信和电话都不要信；不确定时，可拨打航空公司官方客服电话咨询；任何要到ATM机上退票改签的都是骗局。

2. 助学金发放

“XX同学，我是XX教育局的工作人员，现有一项针对贫困学生的助学金，已转入您的个人银行卡，请注意查收。如有疑问，请拨打我省教育厅办公电话XXXXXX。”如果学生通过ATM机转账。在转账过程中，骗子就会以缴纳相关费用为由骗取钱财。所以，接到相关信息，要主动与当地教育部门或学校联系，核实真假。同时不要随意透露家人姓名、电话、职业等信息。

3. 造意外事故

“XX同学家长，我是您孩子的班主任，您的孩子在军训中受伤，需交住院费五千元，请汇入XXXXXX账号。”这类骗子会通过发布招聘信息、引导用户面试、巧立名目收费、恶意毁约等流程诈骗。注意，正规中介或企业不需要缴纳所谓的工号费和保证金。 本报记者 叶薇

4. 猜猜我是谁

“在吗？最近手头有点紧，借点钱吧！”一些冒充熟人的网络视频诈骗，犯罪分子通过盗取图像的方式，用“视频”与你聊天，可千万别上当。

5. 虚假中奖、虚构绑架

骗子冒充苹果、京东商城、电视栏目组等，通过发送虚假中奖信息，说服你交“手续费、保证金、税费”。还有一些电话虚构亲友被绑架，如要解救人质需立即付款到指定账户并不能报警，否则撕票。

6. 网购退款

“您在京东商城有两笔消费，购买了QQ点卡，因为是异地消费，所以我们要确认一下。”这是一种新型诈骗手法。骗子先进入受害人的网银，把钱转到投资账户，这种操作无需任何验证码和手续；下一步，骗子把银行发来的提示信息伪装成有人盗取网银下单，然后伪装成商家骗取受害人的信任；为了博取信任，骗子先从投资账户转小额资金回到网银账户，银行又会发来信息；当受害人信以为真，骗子会以安全为由，让受害人把钱都转移到所谓的“安全账户”里，向受害人索取验证码或让受害人确认支付二维码。一旦完成这一步，骗子即得逞了。

7. 打工兼职

不法分子会通过发布招聘信息、引导用户面试、巧立名目收费、恶意毁约等流程诈骗。注意，正规中介或企业不需要缴纳所谓的工号费和保证金。 本报记者 叶薇

国内首份电信诈骗形势分析报告显示 骗子最爱金融理财类诈骗

本报讯(记者 金志刚)中国最大的互联网安全公司360近日发布了《2016中国电信诈骗形势分析报告》。这也是中国首份基于大数据分析的电信诈骗分析报告。

报告显示，诈骗电话中虚假的金融理财类诈骗最多，占43.2%，此类诈骗在北上广深等大城市尤其盛行；其次是身份冒充诈骗，占25.2%。在身份冒充类诈骗中，冒充电信运营商的诈骗数量最多，占比26.0%；其次是冒充领导，占21.2%；排名第三的是冒充快递，占14.3%。

此外，每周五到下一周的周一，诈骗电话呼叫量相对较高，报告认为造成主要原因在于，周末很多人都会独自在家，有空闲时间，而且身边没有可以给自己提醒的人，被骗子成功诈骗的几率也就更高。在诈骗电话的号码源中，固定电话呼出的诈骗电话数量最多，占所有诈骗电话呼叫量的56.0%；其次是400/800电话，占比为27.1%；手机呼出的诈骗电话占诈骗电话呼叫总量的15.4%；此外，还有1.2%的诈骗电话来自境外呼入。